Amendments to the Claims:

This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims:

1-34. (Canceled)

35. (Previously Presented) A method for preventing a program on a computer from using data transmitted by the computer to a website, comprising:

identifying a first set of codes, each code in the first set of codes associated with a human-readable label for presentation to a user of the computer, the first set of codes including a first code associated with a first human-readable label;

generating a first set of encrypted codes corresponding to the first set of codes, the first set of encrypted codes including a first encrypted code corresponding to the first code, wherein generating the first set of encrypted codes comprises performing an encryption process utilizing a first encryption key identification code;

sending, to the computer, the first set of encrypted codes, the human-readable label associated with each code in the first set of codes, and the first encryption key identification code, wherein the first encryption key identification code is sent concurrently with sending the first set of encrypted codes;

receiving, from the computer, at least one encrypted code from the first set of encrypted codes, and the first encryption key identification code, wherein the at least one encrypted code represents a selection by the user, the received at least one encrypted code includes the first encrypted code, and the first encryption key identification code is received concurrently with receiving the at least one encrypted code from the first set of encrypted codes;

identifying a second set of codes, each code in the second set of codes associated with a human-readable label for presentation to the user of the computer, the second set of codes including the first code;

generating a second set of encrypted codes corresponding to the second set of codes, the second set of encrypted codes including a second encrypted code corresponding to the first code, the second encrypted code different from the first encrypted code, wherein generating the second set of encrypted codes comprises performing the encryption process utilizing a second encryption key identification code different from the first encryption key identification code; and

sending, to the computer concurrently with sending the second set of encrypted codes, the second encryption key identification code.

36-37. (Canceled)

38. (Previously Presented) The method of claim 35, wherein the first encryption key identification code comprises a time stamp, the method further comprising:

evaluating the time stamp to determine whether the received at least one encrypted code from the first set of encrypted codes is valid.

39-42. (Canceled)

43. (Currently Amended) An article comprising a computer-readable storage medium storing instructions for causing a computer system to perform operations to prevent a program on a computer from using data transmitted by the computer to a website, the operations comprising:

generating a first set of encrypted codes corresponding to a first set of codes, the first set of codes including a first code, the first set of encrypted codes including a first encrypted code corresponding to the first code, wherein the first set of encrypted codes is[[are]] associated with a first encryption key identification code, the operations further comprising:

sending, to the computer, the first set of encrypted codes concurrently with the first encryption key identification code;

receiving, from the computer, at least one encrypted code from the first set of encrypted codes concurrently with the first encryption key identification code, the at least one encrypted

code representing a selection by a user of the computer, the received at least one encrypted code including the first encrypted code; and

generating a second set of [[ ]]encrypted codes corresponding to a second set of codes, the second set of codes including the first code, the second set of encrypted codes including a second encrypted code corresponding to the first code, the second encrypted code different from the first encrypted code.

44-47. (Canceled)

48. (Currently Amended) A system for preventing a program on a computer from using data transmitted by the computer to a website, comprising:

a computer system operable to:

identify a set of codes, each code in the set of codes associated with a human-readable label for presentation to a user of the computer, the set of codes including a first code associated with a first human-readable label;

generate a first set of encrypted codes corresponding to a first subset of the set of codes, the first subset including the first code, the first set of encrypted codes including a first encrypted code corresponding to the first code, the first set of encrypted codes associated with an encryption process and a first encryption key identification code, wherein the first encryption key identification code comprises a time stamp indicating when the first set of encrypted codes was created;

send, to the computer, the first set of encrypted codes and the human-readable label associated with each code in the first subset of codes;

receive, from the computer, at least one encrypted code representing a selection by the user, the received at least one encrypted code corresponding to the first code;

generate a first set of decrypted codes corresponding to the received at least one encrypted code, the first set of decrypted codes associated with a decryption process

and the first encryption key identification code, the decryption process comprising the encryption process in reverse;

generate a second set of encrypted codes corresponding to a second subset of the set of codes, the second subset including the first code, the second set of encrypted codes including a second encrypted code corresponding to the first code, the second encrypted code different from the first encrypted code.

49-51. (Canceled)

52. (Previously Presented) The system of claim 48, the computer system further operable to:

compare the time stamp to a predetermined time period; and

determine the validity of the received at least one encrypted code based on the comparison.